8-10-2022

IVLE4C a Conceptual Learning Environment for Teaching Enterprise Cybersecurity

Jeff Greer
University of North Carolina Wilmington, greerj@uncw.edu

Geoff Stoker
University of North Carolina Wilmington, stokerg@uncw.edu

Ulku Yaylacicegi Clark
University of North Carolina Wilmington, clarku@uncw.edu

IVLE4C a Conceptual Learning Environment for Teaching Enterprise Cybersecurity

TREO Talk Paper

Jeff Greer
UNCW
greerj@uncw.edu

Geoff Stoker
UNCW
stokerg@uncw.edu

Dr. Ulku Clark
UNCW
clarku@uncw.edu

Abstract

The authors are working to improve students' understanding of and classroom experience with enterprise cybersecurity. Central to this effort is development of the Integrated Virtual Learning Environment for Cybersecurity (IVLE4C), a teaching and learning tool intended for use by both teachers and students. The authors are endeavoring to incorporate into IVLE4C best practices from the knowledge domains of education, model-based systems engineering, and cybersecurity.

A modern digital enterprise is a large-scale, complex system of systems. Enterprise cybersecurity is a special subset of the larger knowledge domain that merits special consideration when instructing students who lack relevant work experience. This lack of work experience creates a gap in students' knowledge about the structure, operation, and control of a modern digital enterprise.

Our guiding precept – coined Greer's Rule of Thumb – is that: *it is impossible to defend what cannot be visualized and described*. Therefore, it is essential to address the student enterprise knowledge gap before attempting to teach the means for assuring enterprise cybersecurity. Viste and Skartveit (2004) propose using an interactive virtual learning environment with reality abstraction models when teaching the structure, operation, and control of a large-scale complex system. The creation of a virtual model enables a modern digital enterprise to be brought into the classroom. This allows for learning that is complementary to experiential learning that occurs during an internship and, possibly, a viable alternative when internships are unavailable or come later in a curriculum path. Once developed, a library of models representing different digital enterprise types can be used to accelerate student enterprise cybersecurity education in a controlled classroom environment.

During the presentation, the authors will provide an update on the use of model-based system engineering practices and how they are being integrated into IVLE4C for developing a tailored, enterprise risk management strategy. This approach is consistent with guidance provided in the NIST Cybersecurity Framework. Research shows model-based systems engineering is increasingly being used for developing engineered cybersecurity solutions. An example of this is research performed by Robles-Ramirez et.al. (2020) on the application of model-based Cybersecurity Engineering for Connected and Automated Vehicles. Key is the notion of turning a cyber-attack surface into a trust boundary at targeted levels. IVLE4C version 1.0 is currently being used to teach Cyber Supply Chain Security at UNCW. Version 2.0 is a dynamic data driven web application, that is being developed for teaching Enterprise Security.

References

Viste, M., and Skartveit, H, 2004." Visualization of Complex Systems – The Two Shower Model," Psychology Journal, 2004, Volume 2, Number 2, pp. 229-241

Robles-Ramirez, D., et. al. 2020. "Model-based Cybersecurity Engineering for Connected and Automated Vehicles," MBE Summit 2020, NIST